УДК 004.056

АРХИТЕКТУРА ПЛАТФОРМЫ АВТОМАТИЗАЦИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.А. Биюмен, К.Ц. Маршалова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье представлена архитектура платформы для автоматизации аудитов информационной безопасности. Описан подход, объединяющий пассивный сбор данных, копирование веб-ресурсов и фильтрацию машинного трафика. Предложен эвристический алгоритм извлечения персональных данных на основе контекстной близости элементов веб-страниц. Использование микросервисной архитектуры и изолированной маршрутизации обеспечивает объективность оценки устойчивости персонала к целевым атакам методами социальной инженерии.

Ключевые слова: информационная безопасность; социальная инженерия; программная архитектура; пассивный сбор данных; эвристический алгоритм; копирование ресурсов; маршрутизация трафика; фильтрация событий; имитация атак; оценка уязвимостей.

SOFTWARE COMPLEX ARCHITECTURE FOR AUTOMATED INFORMATION SECURITY AUDITS

Y.A. Biyumen, K.C. Marshalava
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article presents a platform architecture for automating information security audits. It describes an approach combining passive data collection, resource copying, and machine traffic filtering. A heuristic algorithm for extracting personal data based on contextual proximity is proposed. Microservice architecture and isolated routing ensure objective assessment of personnel resilience to social engineering attacks.
Keywords: Information security; social engineering; software architecture; passive data collection; heuristic algorithm; resource copying; traffic routing; event filtering; attack simulation; vulnerability assessment.

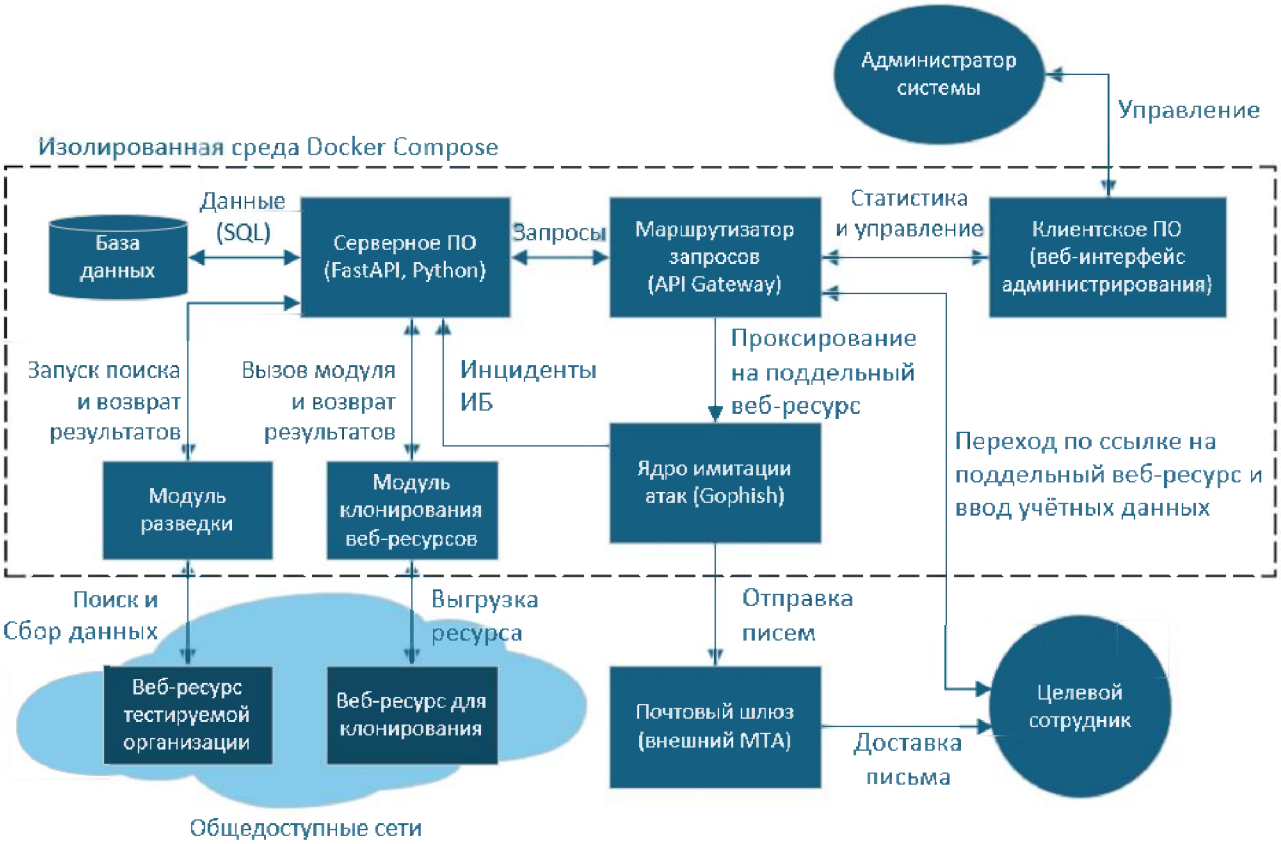
Введение

В 2025–2026 годах социальная инженерия и корпоративный фишинг остаются главными векторами кибератак на организации [1]. Создание поддельных ресурсов для кражи данных является высокоэффективным методом обхода технических средств защиты информации [2]. Противодействие угрозам требует регулярных практических тренировок персонала и превентивного анализа открытых источников [3]. Цель работы – описание архитектуры программной платформы, автоматизирующей полный цикл фишинговых аудитов.

Основная часть

Платформа использует микросервисную архитектуру в изолированной среде контейнеров. Центральным узлом выступает серверное приложение на языке Python. Общая схема архитектуры представлена на рисунке.

Внутренний маршрутизатор выполняет функцию шлюза: управляющий трафик направляется в веб-приложение, а запросы проверяемых сотрудников – на скрытый веб-сервер. Алгоритм фильтрует машинный трафик (от почтовых шлюзов и сканеров), сверяя идентификаторы браузеров и сетевые адреса с известными подсетями анализаторов. Такие автоматические переходы исключаются из итоговой оценки персонала. Реализована ролевая модель доступа к панели администрирования для защиты конфиденциальных данных.



Архитектура программного комплекса
Architecture of the software package

Для создания веб-страниц применяется модуль динамического копирования. Он загружает объектную модель сайта-источника, преобразуя относительные пути к файлам в абсолютные ссылки для корректного отображения. Модуль заменяет оригинальные формы перехватчиками и внедряет скрытые элементы отслеживания действий.

Сбор данных осуществляет модуль автоматизированной разведки. Программа-обходчик анализирует корпоративный сайт исключительно по навигационным маркерам контактов. Извлекая адреса электронной почты, алгоритм выделяет фрагмент текста (200 символов) и ищет последовательности из трех слов с прописной буквы (потенциальные ФИО). Применяя словари исключений и механизм негативного контекста, система отсеивает адреса и должности. При нахождении нескольких вариантов (потенциальных ФИО) вычисляется количество символов (дистанция) в HTML-коде до адреса электронной почты, после чего алгоритм связывает почту с ближайшим текстовым значением. Это автоматизирует формирование целевой базы.

Выполнение рассылок возложено на изолированное ядро. Оно формирует письма по шаблонам, доставляет их с подстановкой персональных данных и фиксирует этапы взаимодействия (доставка,

открытие, ввод данных), передавая события в главную базу для анализа метрик и формирования отчета.

Заключение

Разработанная платформа объединяет пассивный сбор данных, копирование ресурсов, рассылку и фильтрацию статистики. Выбранная архитектура значительно сокращает время подготовки аудитов информационной безопасности и предоставляет метрики уязвимости персонала. Дальнейшее развитие предполагает внедрение машинного обучения для обработки естественного языка, интеграцию собственного отказоустойчивого модуля отправки писем и улучшение алгоритмов копирования современных одностраничных веб-приложений.

Список использованных источников

1. Диреев И. Д. (2025) Социальная инженерия в контексте информационной безопасности. Международный научно-исследовательский журнал. (3), 39–46.
2. Гордиенко В. В., Жданов Д. М. (2024) Методы защиты от социальной инженерии и фишинга. Их достоинства и недостатки. Auditorium. (2), 45-49.
3. Туманов Е. М. (2025) Методы анализа информационной безопасности организации с использованием OSINT. Вестник науки. (5), 926–933.

References

1. Direev I. D. (2025) Social Engineering in the Context of Information Security. International Research Journal. (3), 39–46.
2. Gordienko V. V., Zhdanov D. M. (2024) Methods of Protection Against Social Engineering and Phishing. Their Advantages and Disadvantages. Auditorium. (2), 45–49.
3. Tumanov E. M. (2025) Methods of Analyzing Organization's Information Security Using OSINT. Vestnik Nauki. (5), 926–933.

Сведения об авторах

Биюмен Е.А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», eugene.aether@gmail.com.

Маршалова К.Ц., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», krissmarshalova@gmail.com.

Information about the authors

Biyumen Y., student of Information Security Faculty, Educational Institution "Belarusian State University of Informatics and Radioelectronics", eugene.aether@gmail.com.

Marshalava K., student of Information Security Faculty, Educational Institution "Belarusian State University of Informatics and Radioelectronics", krissmarshalova@gmail.com.